REMARKS

In view of the following discussion, the Applicants submit that none of the claims now pending in the application are obvious under the provisions of 35 U.S.C. § 103. Thus, the Applicants believe that all of these claims are now in allowable form.

I. AMENDMENT TO THE SPECIFICATION

The Examiner has objected to the specification because the abstract of the disclosure exceeds 150 words in length. In response, the Applicants have amended the specification. Namely, the abstract has been amended such that the 150 word limitation is not exceeded. As such, the Applicants respectfully request the objection be withdrawn.

II. REJECTION OF CLAIMS 1-11 UNDER 35 U.S.C. § 103

A. Claims 1-4 and 6-9

The Examiner has rejected claims 1-4 and 6-9 in the Office Action under 35 U.S.C. § 103 as being unpatentable over DeTreville (US Patent 6,609,199, issued August 19, 2003, hereinafter referred to as "DeTreville") in view of Schneier, et al. (US Patent 5,768,382, issued June 16, 1998, hereinafter referred to as "Schneier") and Fielder, et al. (US Patent 6,105,133, issued August 15, 2000, hereinafter referred to as "Fielder"). Applicants respectfully traverse the rejection.

DeTreville teaches a method and apparatus for authenticating an open system application to a portable IC device. The IC device allows users to access private information on another computer from an open system (see DeTreville, Col. 4, Lines 18-27). The IC device authenticates itself, the user, and any applications running on the open system to ensure the applications can be trusted (see *Id.* at Lines 35-46).

Schneier teaches a remote-auditing of computer generated outcomes and authenticated billing and access control system using cryptographic and other protocols. Schneier allows for secure tracking of computer game outcomes (see Schneier, Abstract).

Fielder teaches a bilateral authentication and encryption system. The system involves a static secret and a dynamic secret (see Fielder, Col. 2, Lines 60-67). Both

the static and dynamic secrets are stored on a hard drive and placed into RAM during authentication (see Fielder, Col. 4, Line 59 - Col. 5 Line 4). After the session is over the RAM is either overwritten or erased and the new dynamic secret is stored on the hard drive (see *Id).*

The Examiner's attention is directed to the fact that DeTreville, Schneier and Fielder, individually or in any permissible combination, fail to teach, show or suggest a persistent memory element that contains second information to enable the security mechanism to configure the network peripheral device to access different networks, as positively claimed by Applicants' amended independent claim 1. Specifically, Applicants' independent claim 1 recites:

> 1. A security mechanism for enabling a user to commence a session between a network peripheral device and a network, comprising:
> an immutable memory element that contains first information including application software that initiates and provides security services;
> a persistent memory element that contains second information to enable the security mechanism to configure the network peripheral device to access different networks;
> a volatile memory element that contains third information, including the critical data for authentication, said third information erased from the volatile memory at the completion of each connection session; and
> a tamper-evident enclosure for enclosing the memory elements.
> (Emphasis Added)

Applicants' invention teaches the novel concept of a security mechanism that has a persistent memory element that contains second information to enable the security mechanism to configure the network peripheral device to access different networks. Applicants' invention advantageously allows a device to be configured to access any network and the corresponding network's software (see Applicants' Specification, Page 3, Lines 16-17; Page 6, lines 6-9 of Paragraph [0013]). In other words, the same laptop, for example, can be connected to various networks.

In contrast, DeTreville, Schneier and Fielder, individually or in any permissible combination fail to teach, show or suggest the Applicants' invention. DeTreville only teaches an IC device that authenticates and secures the computer on an open system it is connected to (see DeTreville, Col. 5, Lines 13-34). DeTreville's invention is limited in

that the IC device cannot configure a security mechanism to work in various networks, as in the Applicants' invention. The IC device is intended to contain information that proves that the IC unit is present relative to the open system computer (see DeTreville, Column 4, lines 35-38). The same is true in Schneier and Fielder. Schneier only teaches secure tracking of computer game outcomes (see Schneier, Abstract). Finally, Fielder is only concerned with the encryption and authentication between computers on the same communication link (see Fielder, Col. 4, Lines 20-28). Fielder does not teach, show or suggest that the same computer can communicate over various networks. In summary, the Examiner's attention is directed to the fact that, unlike the Applicants' invention that allows a security mechanism to configure the network peripheral device to access different networks, DeTreville, Schneier and Fielder's security mechanisms are all limited to the existing network protocol the computers are communicating over. Therefore, the combination of DeTreville, Schneier and Fielder does not teach or suggest Applicants' invention as recited in independent claim 1.

In rejecting claims under 35 U.S.C. §103, it is incumbent upon the Examiner to establish a factual basis to support the legal conclusion of obviousness. See In re Fine, 837 F.2d 1071, 1073, 5 USPQ2d 1596, 1598 (Fed. Cir. 1988). In so doing, the Examiner is expected to make the factual determinations set forth in Graham v. John Deere Co., 383 U.S. 1, 17, 148 USPQ 459, 467 (1966), and to provide a reason why one having ordinary skill in the pertinent art would have been led to modify the prior art or to combine prior art references to arrive at the claimed invention. Such reason must stem from some teaching, suggestion or implication in the prior art as a whole or knowledge generally available to one having ordinary skill in the art. Uniroyal, Inc. v. Rudkin-Wiley Corp., 837 F.2d 1044, 1051, 5 USPQ2d 1434, 1438 (Fed. Cir), cert. denied, 488 U.S. 825 (1988); Ashland Oil, Inc. v. Delta Resins & Refractories, Inc., 776 F.2d 281 293, 227 USPQ 657, 664 (Fed. Cir. 1985), cert. Denied, 475 U.S. 1017 (1986); ACS Hosp. Sys., Inc. v. Montefiore Hosp. 732 F.2d 1572, 1577, 221 USPQ 929, 933 (Fed. Cir. 1984). These showings by the Examiner are an essential part of complying with the burden of presenting a prima facie case of obviousness. Note In re Oetiker, 977 F.2d 1443, 1445, 24 USPQ2d 1443, 1444 (Fed. Cir. 1992). Applicants

submit that the Examiner failed to present a prima facie case in rejecting Applicants' independent claims.

Dependent claims 2-4 and 6-9 depend, either directly or indirectly, from independent claim 1 and recite additional limitations. As such, and for the exact same reason set forth above, the Applicants submit that claims 2-4 and 6-9 are also not made obvious by the teachings of DeTreville, Schneier and Fielder. As such, the Applicants respectfully request the rejection be withdrawn.

B. Claim 5

The Examiner has rejected claim 5 in the Office Action under 35 U.S.C. § 103 as being unpatentable over DeTreville in view of Schneier and Fielder and further in view of Borza (US Patent 6,721,891, Issued April 13, 2004, hereinafter referred to as "Borza"). Applicants respectfully traverse the rejection.

The teachings of DeTreville, Schneier and Fielder have been discussed above. Borza teaches a method of distributing piracy protected computer software. Borza teaches a method and system for disabling execution of a software application stored within a computer absent data indicative of an authorized use of the software application (see Borza, Abstract).

As stated above, the Examiner's attention is directed to the fact that DeTreville, Schneier, Fielder and Borza, individually or in any permissible combination, fail to teach, show or suggest a persistent memory element that contains second information to enable the security mechanism to configure the network peripheral device to access different networks, as positively claimed by Applicants' independent claim 1 (see *supra*).

Applicants' invention teaches the novel concept of a security mechanism that has a persistent memory element that contains second information to enable the security mechanism to configure the network peripheral device to different networks. The Applicants' invention advantageously allows a device to be configured to any network and the corresponding networks software (see Applicants' Specification, Page 3, Lines 16-17; Page 6, Lines 6-9 of Paragraph [0013]). In other words, the same laptop, for example, can be connected to various networks.

In contrast, DeTreville, Schneier and Fielder, individually or in any permissible

combination fail to teach, show or suggest the Applicants' invention. DeTreville only teaches an IC device that authenticates and secures the computer on an open system it is connected to (see DeTreville, Col. 5, Lines 13-34). DeTreville's invention is limited in that the IC device cannot configure a security mechanism to work in various networks, as in the Applicants' invention. Schneier only teaches secure tracking of computer game outcomes. Fielder is only concerned with the encryption and authentication between computers on the same communication link (see Fielder, Col. 4, Lines 20-28). Fielder does not teach, show or suggest that the same computer can communicate over various networks. In summary, the Examiner's attention is directed to the fact that, unlike the Applicants' invention that allows a security mechanism to configure the network peripheral device to access different networks, DeTreville, Schneier and Fielder's security mechanisms are all limited to the existing network protocol the computers are communicating over.

Borza fails to bridge the substantial gap left by DeTreville, Schneier and Fielder. Borza only teaches a method and system for disabling execution of a software application stored within a computer absent data indicative of an authorized use of the software application (see Borza, Abstract). Borza is completely void of any teachings of a security mechanism to configure the network peripheral device to access different networks, as taught by the Applicants' invention. As such, the combination of DeTreville, Schneier, Fielder and Borza clearly does not teach or suggest Applicants' invention as recited in independent claim 1.

Dependent claim 5 depends indirectly from independent claim 1 and recites additional limitations. As such, and for the exact same reason set forth above, the Applicants submit that claim 5 is also not made obvious by the teachings of DeTreville, Schneier, Fielder and Borza. As such, the Applicants respectfully request the rejection be withdrawn.

C. Claims 10 and 11

The Examiner has rejected claims 10 and 11 in the Office Action under 35 U.S.C. § 103 as being unpatentable over DeTreville in view of Fielder. Applicants respectfully traverse the rejection.

The teachings of DeTreville and Fielder have been discussed above. The Examiner's attention is directed to the fact that DeTreville and Fielder, individually or in any permissible combination, fail to teach, show or suggest a method for facilitating a secure connection session with a user between a network peripheral device and a network that includes the step of accessing a persistent memory element that contains second information including configuration information to enable the security mechanism to configure the network peripheral device to access the network, as positively claimed by Applicants amended independent claim 10. Specifically, Applicants' independent claim 10 recites:

> 10. A method for facilitating a secure connection session with a user between a network peripheral device and a network, comprising the steps of:
> accessing an immutable memory element that contains first information that provides security services;
> accessing a persistent memory element that contains second information including configuration information to enable the security mechanism to configure the network peripheral device to access a network;
> accessing a volatile memory element that contains third information, including the critical data for authentication; and
> erasing said third information not later than the end of the connection session so no third information remains in the volatile memory between sessions. (Emphasis Added)

Applicants' invention teaches a method for facilitating a secure connection session with a user between a network peripheral device and a network that includes the step of accessing a persistent memory element that contains second information including configuration information to enable the security mechanism to configure the network peripheral device to access the network. The Applicants' method advantageously allows a device to be configured to access any network and the corresponding networks software (see Applicants' Specification, Page 3, Lines 16-17; Page 6, Lines 6-9 of Paragraph [0013]). In other words, the same laptop, for example, can be connected to various networks.

In contrast, DeTreville and Fielder, individually or in any permissible combination fail to teach, show or suggest the Applicants' method. DeTreville only teaches an IC device that authenticates and secures the computer on an open system it is connected

to (see DeTreville, Col. 5, Lines 13-34). DeTreville's invention is limited in that the IC device cannot configure a security mechanism to work in various networks, as in the Applicants' method. Fielder is only concerned with the encryption and authentication between computers on the same communication link (see Fielder, Col. 4, Lines 20-28). Fielder does not teach, show or suggest that the same computer can communicate over various networks. In summary, the Examiner's attention is directed to the fact that, unlike the Applicants' method that accesses a persistent memory element that contains configuration information to enable a security mechanism to configure the network peripheral device to access a network, DeTreville and Fielder's security mechanisms are all limited to the existing network protocol the computers are communicating over. Therefore, the combination of DeTreville and Fielder does not teach or suggest Applicants' method as recited in independent claim 10.

Dependent claim 11 depends from independent claim 10 and recites additional limitations. As such, and for the exact same reason set forth above, the Applicants submit that claim 11 is also not made obvious by the teachings of DeTreville and Fielder. As such, the Applicants respectfully request the rejection be withdrawn.

Conclusion

Thus, the Applicants submit that all of these claims now fully satisfy the requirement of 35 U.S.C. §103. Consequently, the Applicants believe that all these claims are presently in condition for allowance. Accordingly, both reconsideration of this application and its swift passage to issue are earnestly solicited.

If, however, the Examiner believes that there are any unresolved issues requiring the issuance of a final action in any of the claims now pending in the application, it is requested that the Examiner telephone Mr. Kin-Wah Tong, Esq. at (732) 530-9404 so that appropriate arrangements can be made for resolving such issues as expeditiously as possible.

Respectfully submitted,

9/29/05

Patterson & Sheridan, LLP
595 Shrewsbury Avenue
Shrewsbury, New Jersey 07702

Kin-Wah Tong, Attorney
Reg. No. 39,400
(732) 530-9404